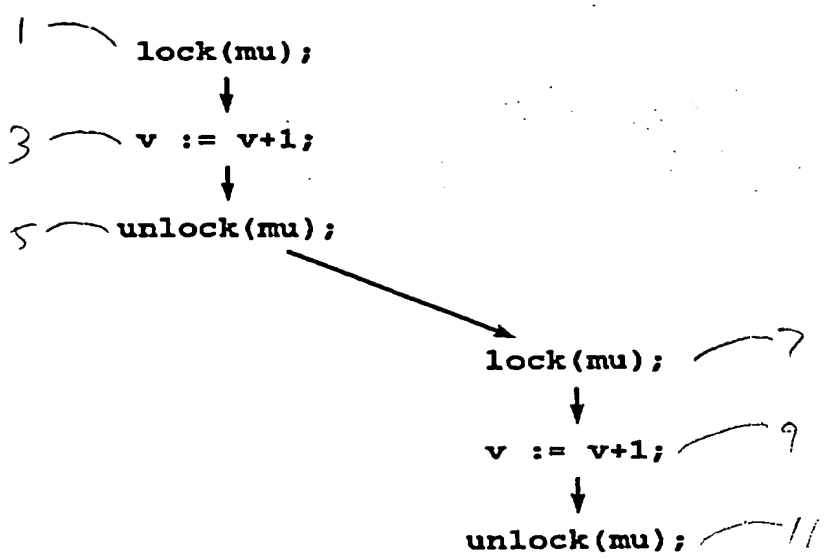

FIG. 1

	Program	*locks_held*	*C(v)*
		{}	{mu1,mu2}
101	lock(mu1);	{mu1}	
103	v := v+1;		{mu1}
105	unlock(mu1);	{}	
107	lock(mu2);	{mu2}	
109	v := v+1;		{}
111	unlock(mu2);	{}	

FIG. 2

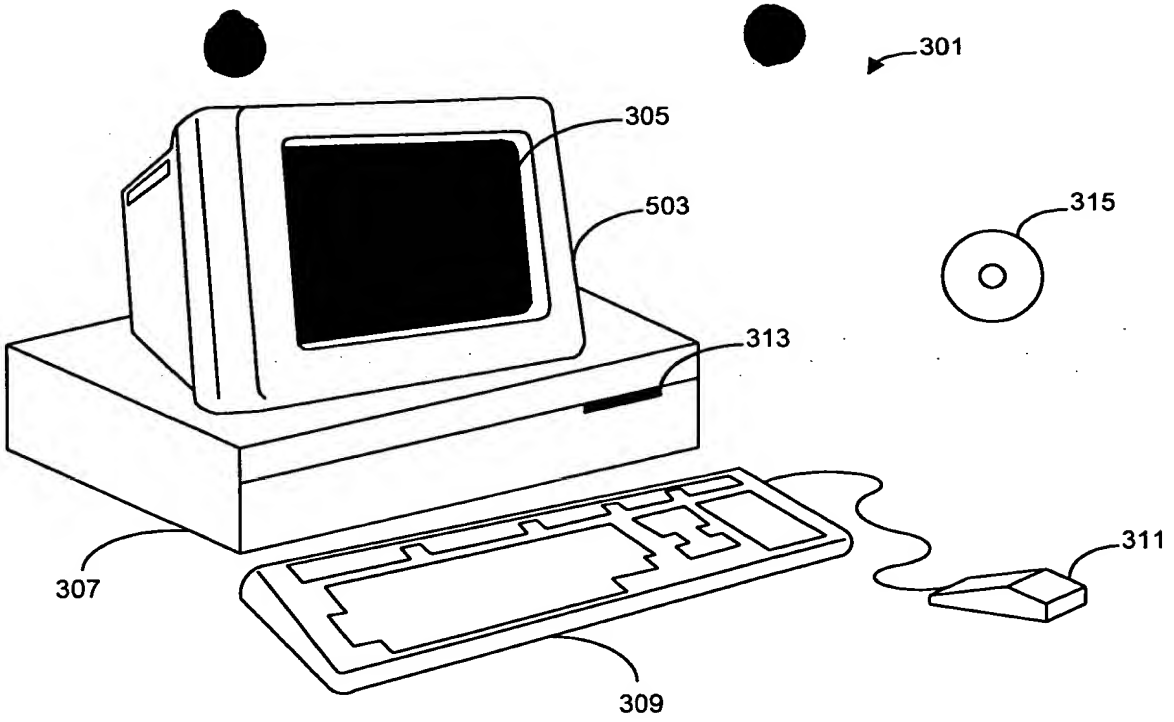
301
305
503
315
313
307
311
309

FIG. 3

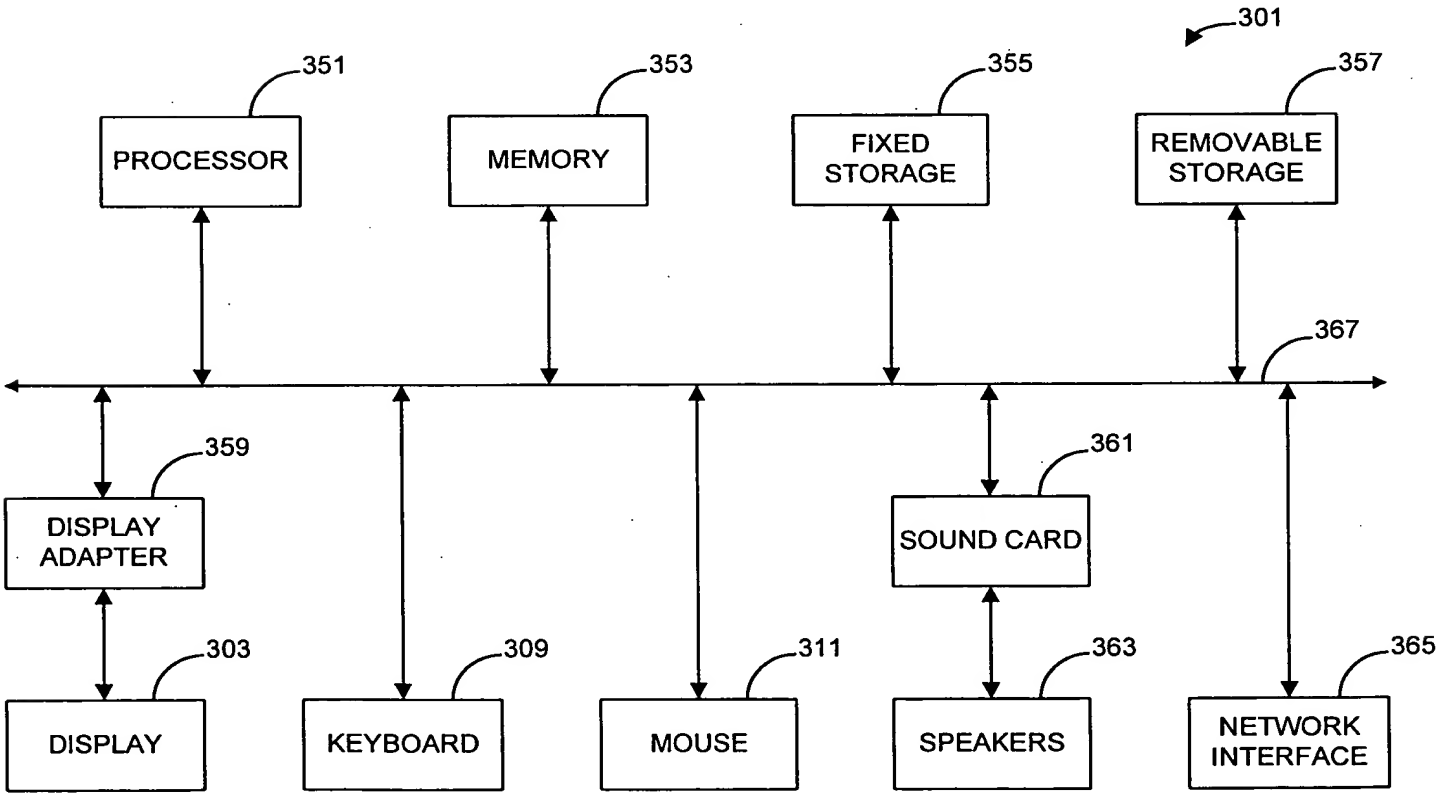
301
351
353
355
357
PROCESSOR
MEMORY
FIXED STORAGE
REMOVABLE STORAGE
367
359
361
DISPLAY ADAPTER
SOUND CARD
303
309
311
363
365
DISPLAY
KEYBOARD
MOUSE
SPEAKERS
NETWORK INTERFACE

FIG. 4

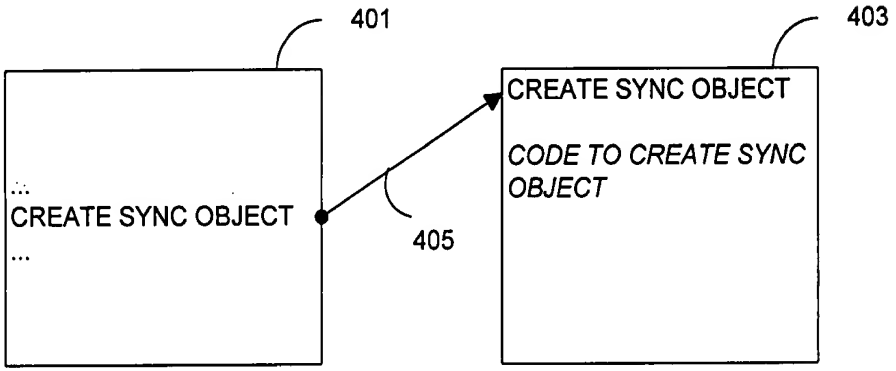

FIG. 5A

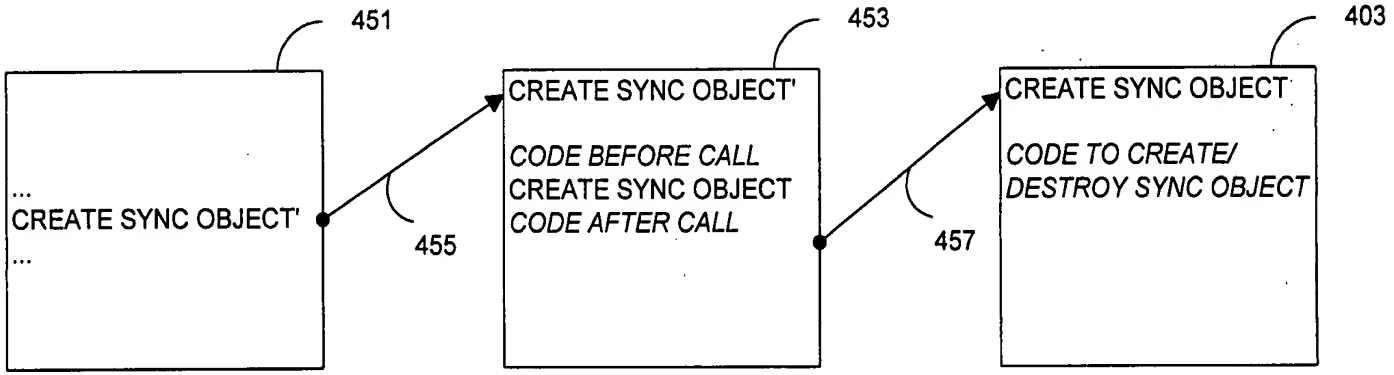

FIG. 5B

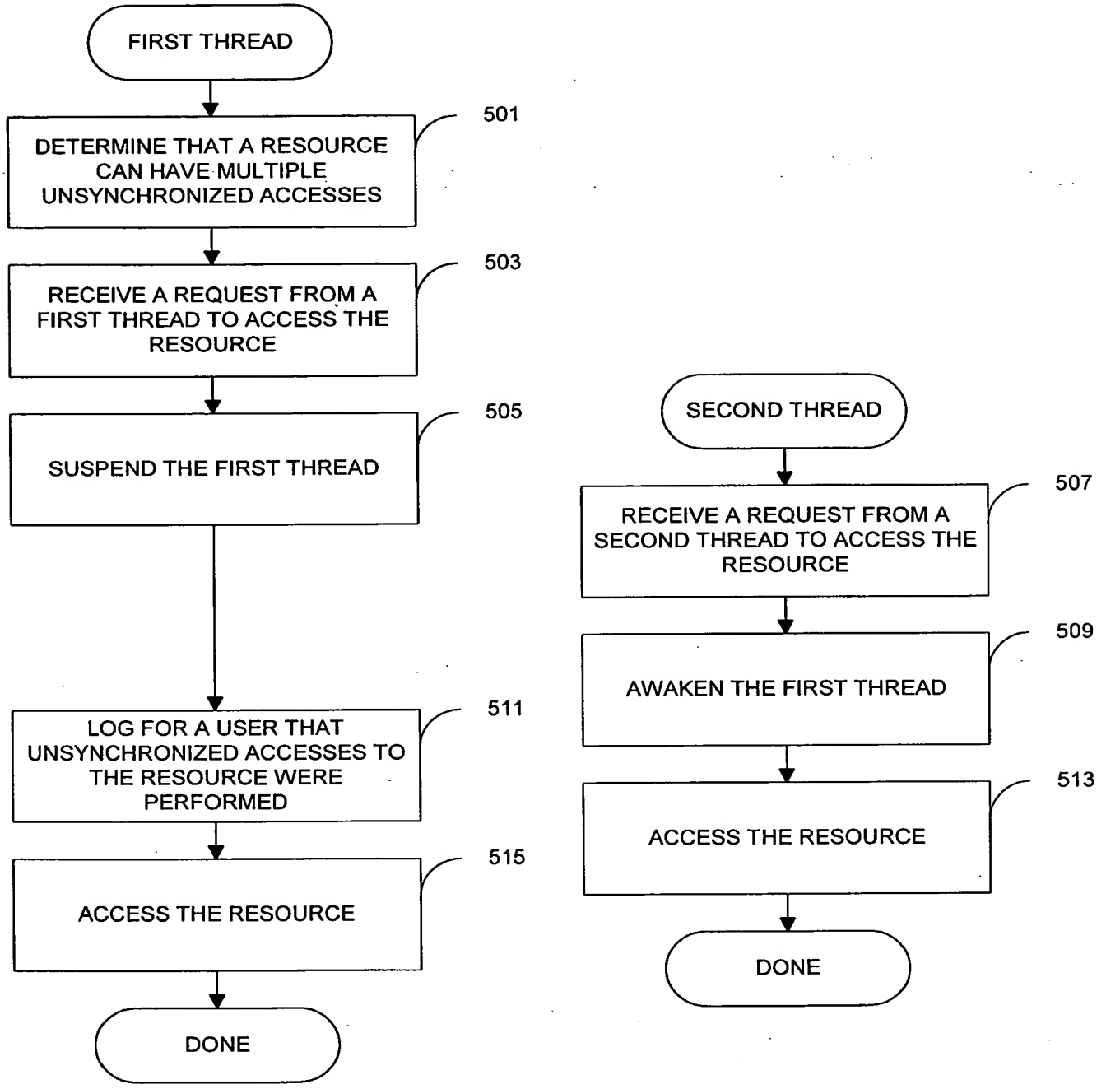
FIRST THREAD
DETERMINE THAT A RESOURCE CAN HAVE MULTIPLE UNSYNCHRONIZED ACCESSES
501
RECEIVE A REQUEST FROM A FIRST THREAD TO ACCESS THE RESOURCE
503
SUSPEND THE FIRST THREAD
505
LOG FOR A USER THAT UNSYNCHRONIZED ACCESSES TO THE RESOURCE WERE PERFORMED
511
ACCESS THE RESOURCE
515
DONE
SECOND THREAD
RECEIVE A REQUEST FROM A SECOND THREAD TO ACCESS THE RESOURCE
507
AWAKEN THE FIRST THREAD
509
ACCESS THE RESOURCE
513
DONE

FIG. 6

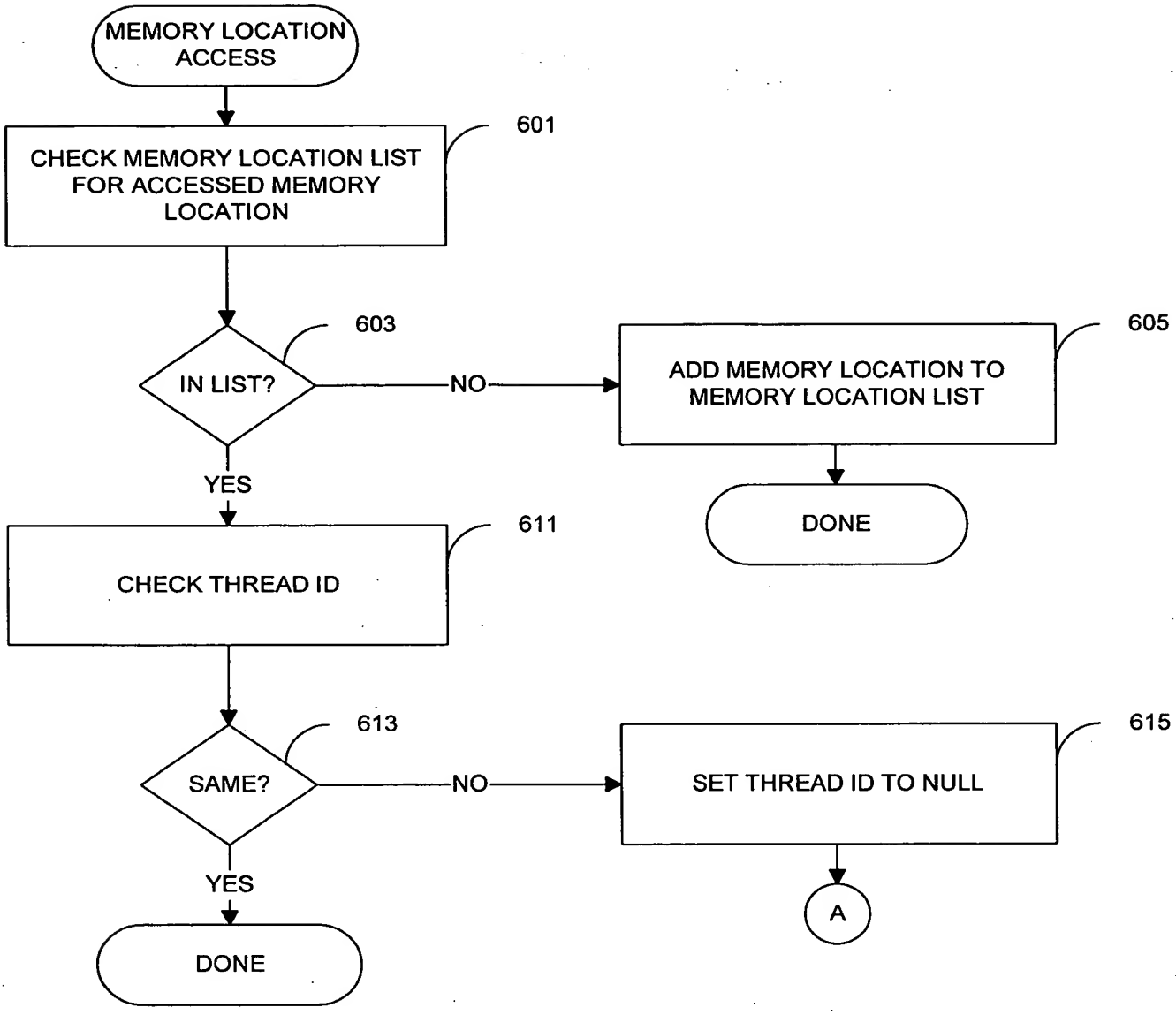
MEMORY LOCATION ACCESS
CHECK MEMORY LOCATION LIST FOR ACCESSED MEMORY LOCATION
601
IN LIST?
603
NO
ADD MEMORY LOCATION TO MEMORY LOCATION LIST
605
DONE
YES
CHECK THREAD ID
611
SAME?
613
NO
SET THREAD ID TO NULL
615
A
YES
DONE

FIG. 7A

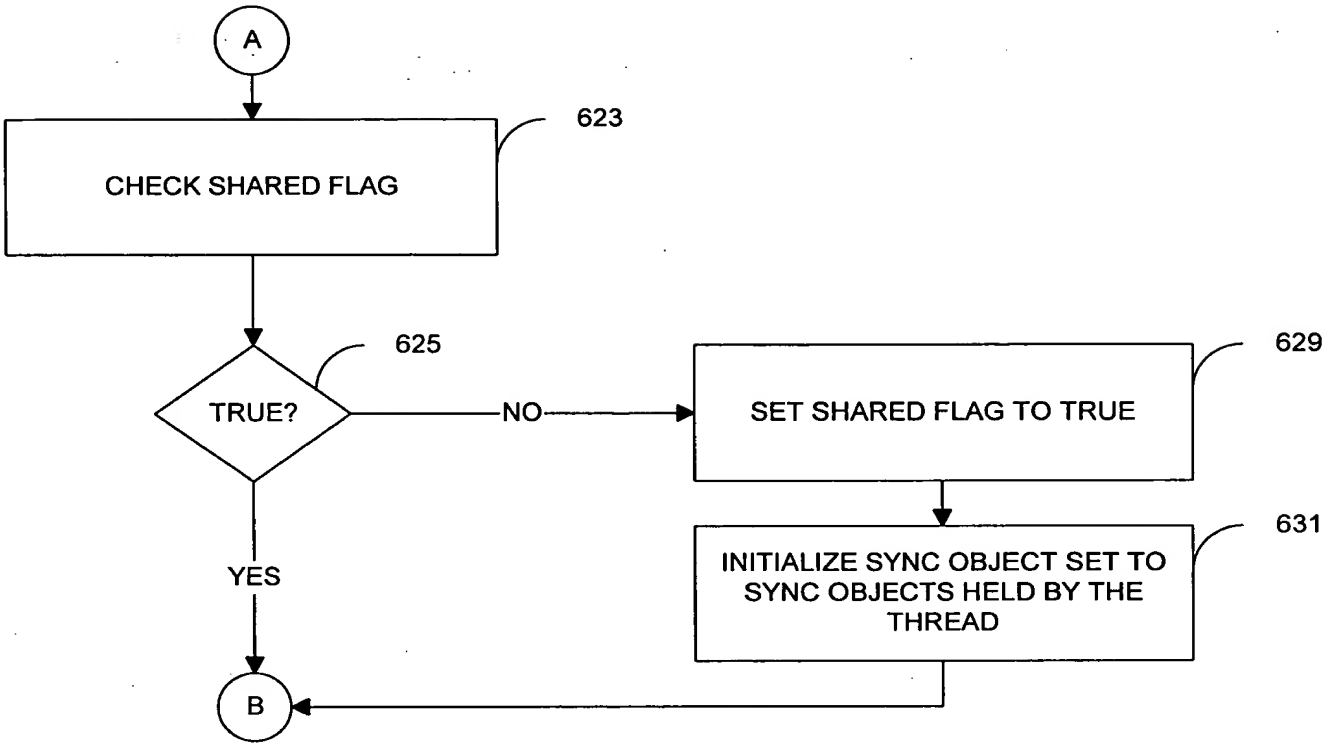
A
CHECK SHARED FLAG
623
625
TRUE?
NO
SET SHARED FLAG TO TRUE
629
631
INITIALIZE SYNC OBJECT SET TO SYNC OBJECTS HELD BY THE THREAD
YES
B

FIG. 7B

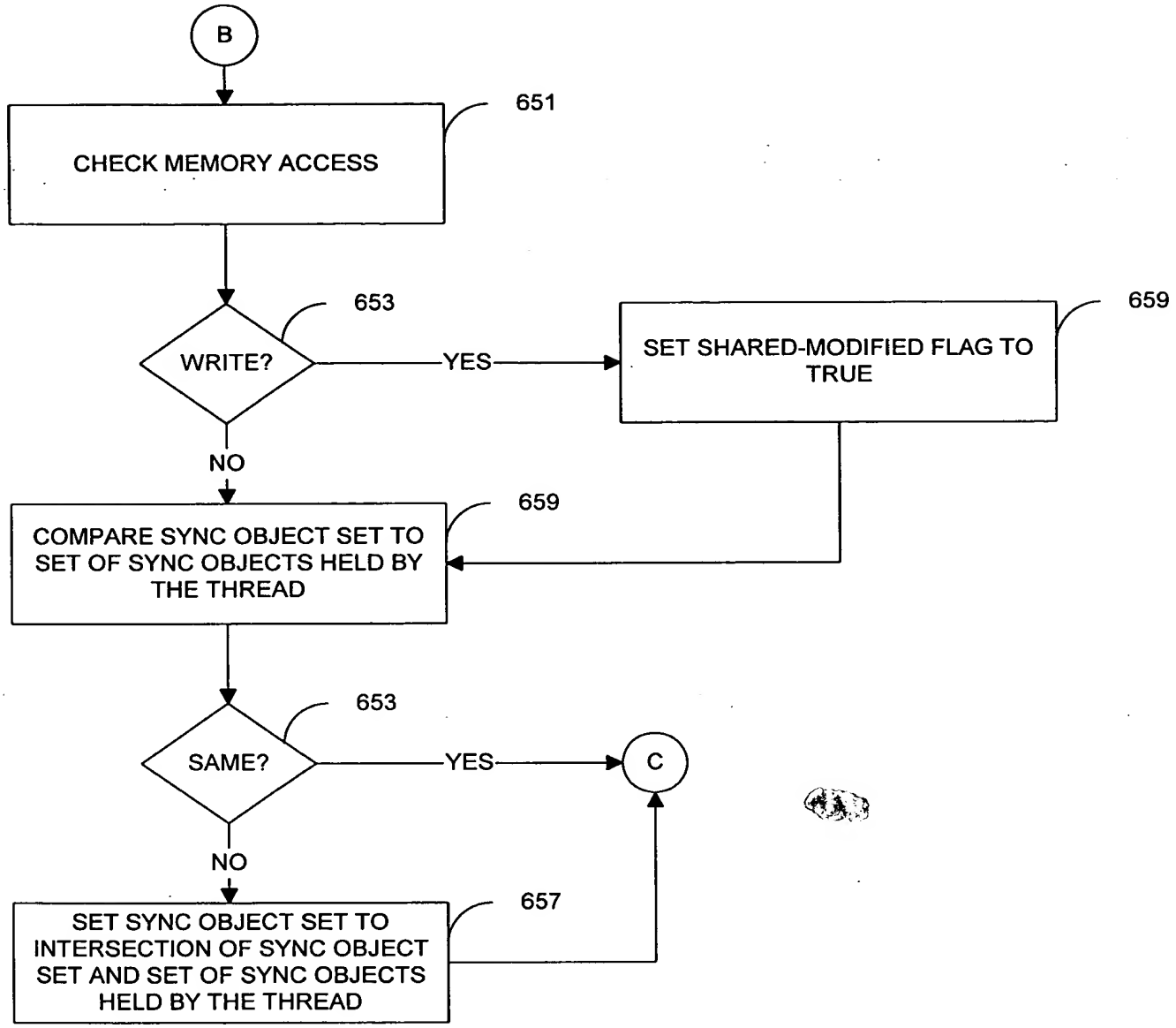
B
CHECK MEMORY ACCESS
651
WRITE?
653
YES
SET SHARED-MODIFIED FLAG TO TRUE
659
NO
COMPARE SYNC OBJECT SET TO SET OF SYNC OBJECTS HELD BY THE THREAD
659
SAME?
653
YES
C
NO
SET SYNC OBJECT SET TO INTERSECTION OF SYNC OBJECT SET AND SET OF SYNC OBJECTS HELD BY THE THREAD
657

FIG. 7C

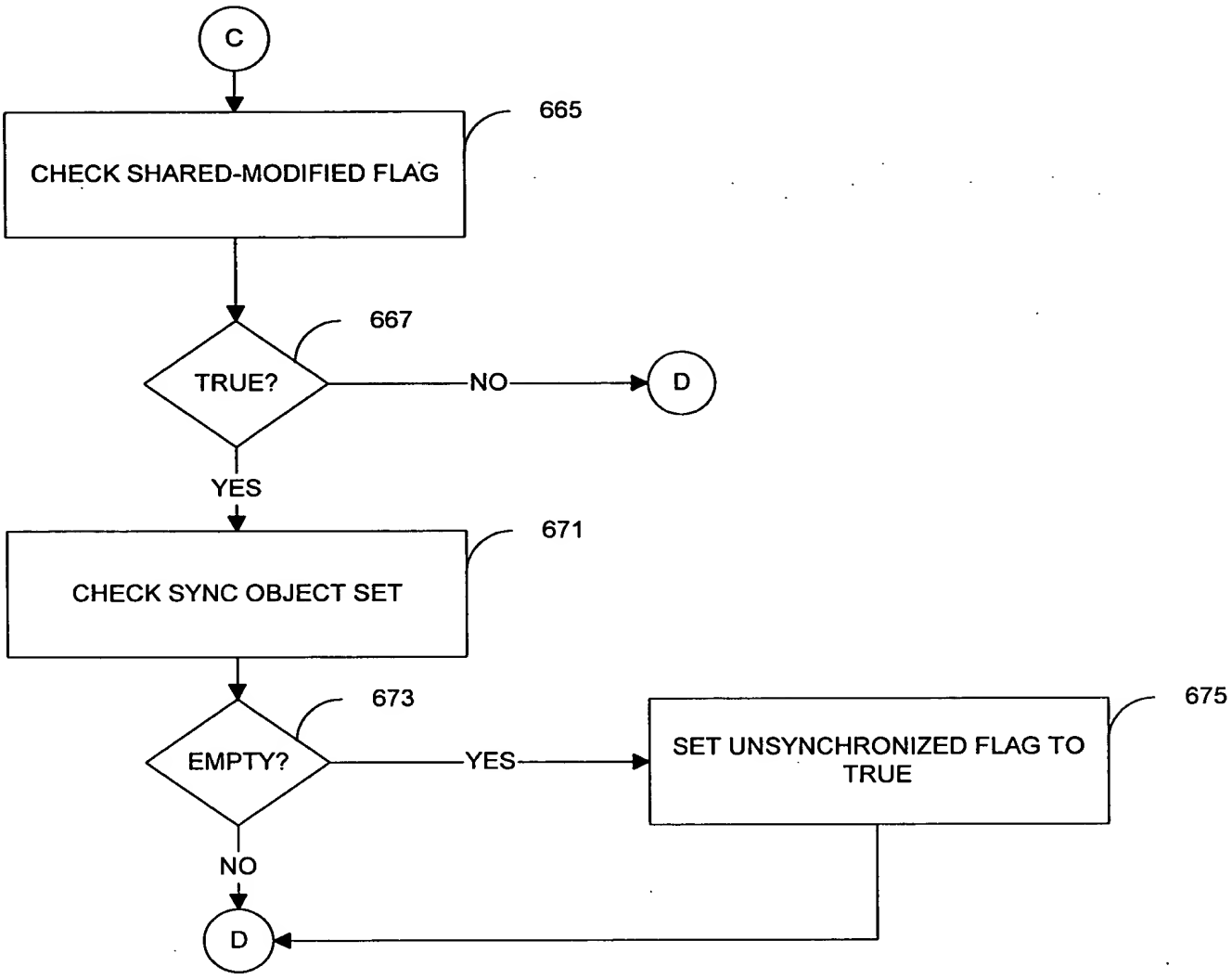
C
665
CHECK SHARED-MODIFIED FLAG
667
TRUE?
NO
D
YES
671
CHECK SYNC OBJECT SET
673
EMPTY?
YES
675
SET UNSYNCHRONIZED FLAG TO TRUE
NO
D

FIG. 7D

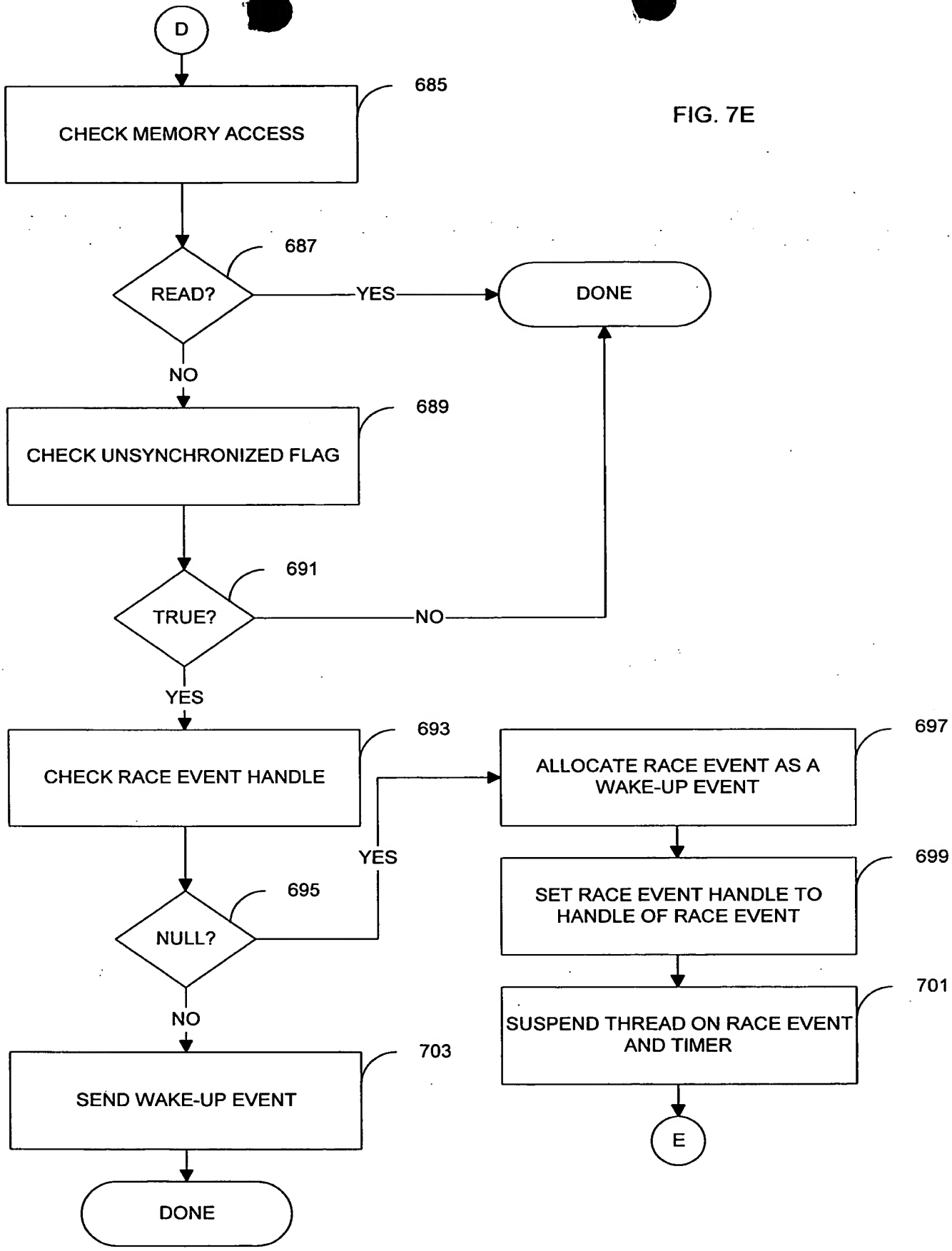
D
CHECK MEMORY ACCESS
685
READ?
687
YES
DONE
NO
CHECK UNSYNCHRONIZED FLAG
689
TRUE?
691
NO
YES
CHECK RACE EVENT HANDLE
693
NULL?
695
YES
NO
SEND WAKE-UP EVENT
703
DONE
ALLOCATE RACE EVENT AS A WAKE-UP EVENT
697
SET RACE EVENT HANDLE TO HANDLE OF RACE EVENT
699
SUSPEND THREAD ON RACE EVENT AND TIMER
701
E

FIG. 7E

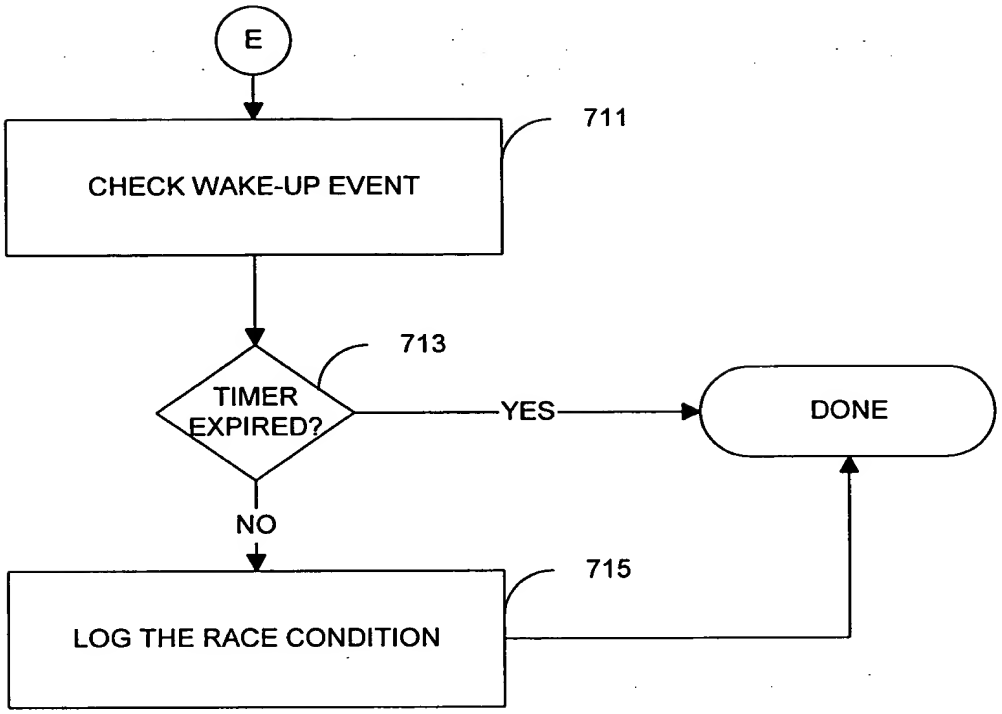
E
711
CHECK WAKE-UP EVENT
713
TIMER EXPIRED?
YES
DONE
NO
715
LOG THE RACE CONDITION

FIG. 7F

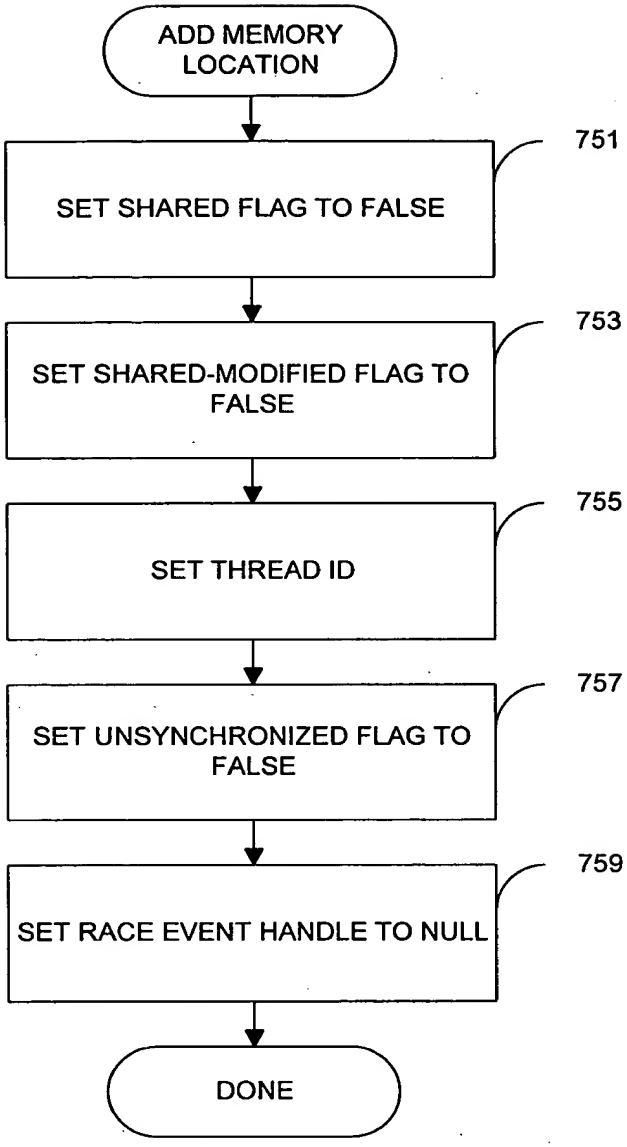
ADD MEMORY LOCATION
751
SET SHARED FLAG TO FALSE
753
SET SHARED-MODIFIED FLAG TO FALSE
755
SET THREAD ID
757
SET UNSYNCHRONIZED FLAG TO FALSE
759
SET RACE EVENT HANDLE TO NULL
DONE

FIG. 8

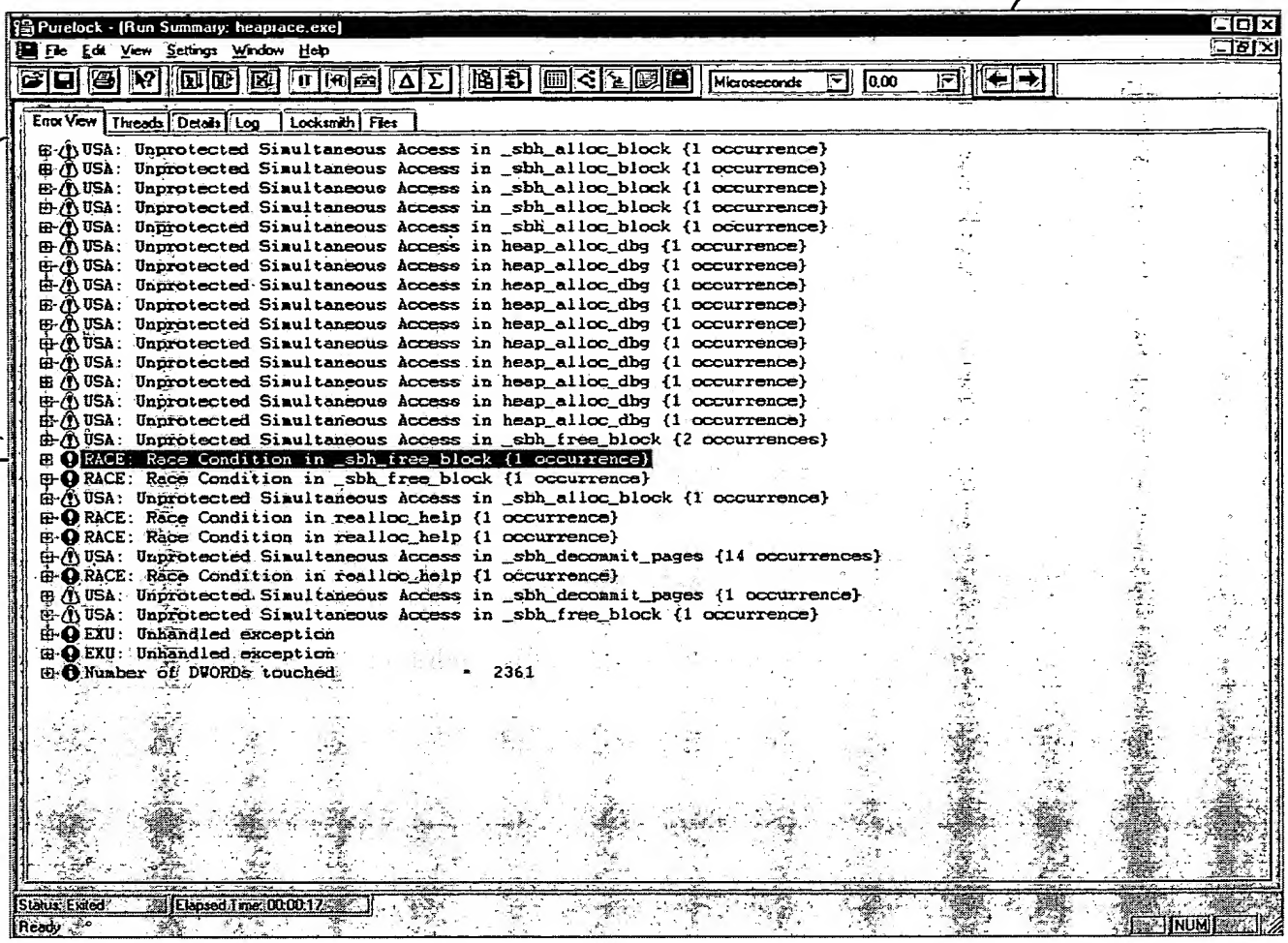
901
Purelock - [Run Summary: heaprace.exe]
File Edit View Settings Window Help
Microseconds
0.00
Error View
Threads
Details
Log
Locksmith
Files
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_free_block {2 occurrences}
RACE: Race Condition in _sbh_free_block {1 occurrence}
RACE: Race Condition in _sbh_free_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
RACE: Race Condition in realloc_help {1 occurrence}
RACE: Race Condition in realloc_help {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_decommit_pages {14 occurrences}
RACE: Race Condition in realloc_help {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_decommit_pages {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_free_block {1 occurrence}
EXU: Unhandled exception
EXU: Unhandled exception
Number of DWORDs touched = 2361
Status: Exited
Elapsed Time: 00:00:17
Ready
NUM
703
905

FIG. 9

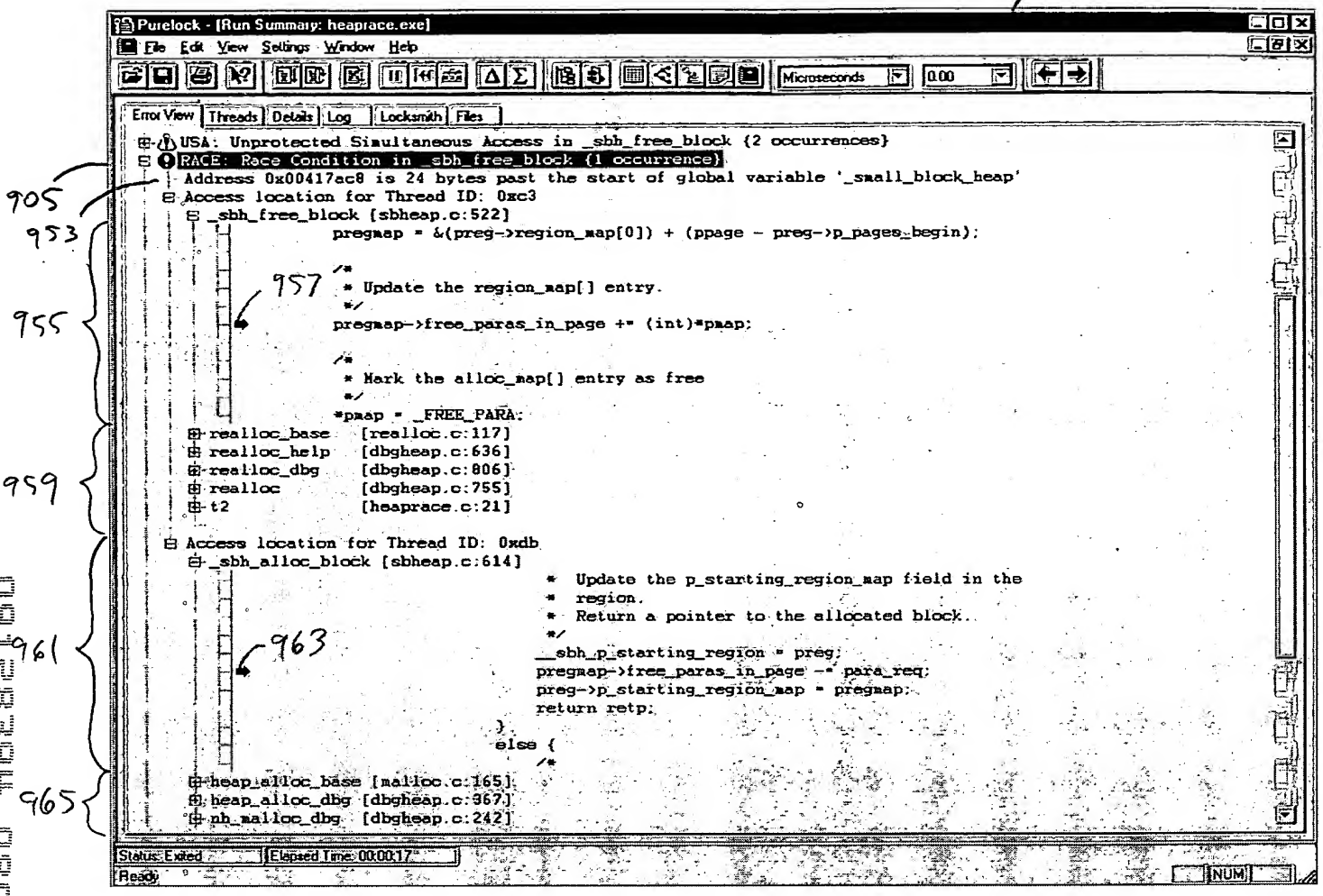
951
Purelock - [Run Summary: heaprace.exe]
File Edit View Settings Window Help
Microseconds
0.00
Error View
Threads
Details
Log
Locksmith
Files
USA: Unprotected Simultaneous Access in _sbh_free_block (2 occurrences)
RACE: Race Condition in _sbh_free_block (1 occurrence)
Address 0x00417ac8 is 24 bytes past the start of global variable '_small_block_heap'
Access location for Thread ID: 0xc3
_sbh_free_block [sbheap.c:522]
pregmap = &(preg->region_map[0]) + (ppage - preg->p_pages_begin);
/*
* Update the region_map[] entry.
*/
pregmap->free_paras_in_page += (int)*pmap;
/*
* Mark the alloc_map[] entry as free
*/
*pmap = _FREE_PARA;
realloc_base [realloc.c:117]
realloc_help [dbgheap.c:636]
realloc_dbg [dbgheap.c:806]
realloc [dbgheap.c:755]
t2 [heaprace.c:21]
Access location for Thread ID: 0xdb
_sbh_alloc_block [sbheap.c:614]
* Update the p_starting_region_map field in the
* region.
* Return a pointer to the allocated block.
*/
__sbh_p_starting_region = preg;
pregmap->free_paras_in_page -= para_req;
preg->p_starting_region_map = pregmap;
return retp;
}
else {
/*
heap_alloc_base [malloc.c:165]
heap_alloc_dbg [dbgheap.c:967]
nh_malloc_dbg [dbgheap.c:242]
Status: Exited
Elapsed Time: 00:00:17
Ready
NUM
905
953
957
955
959
961
963
965

FIG. 10